zkMe Technology Limited Entity NO.: 74666593-000-12-22-5
21/B, Hoi On Commercial Building
8 Mui Fong Street, Sai Ying Pun
Hong Kong
(852) 5717 7263
contact@zk.me

Re: Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators licensed by the Securities and Futures Commission

March 28th, 2023

Securities and Futures Commission
54/F, One Island East
18 Westlands Road, Quarry Bay
Hong Kong

To whom it may concern,

We at zkMe appreciate the opportunity to respond to the consultation paper on the regulatory requirements for VATPs licensed by the SFC. Our startup company operates as a KYC SaaS provider specializing in serving the market of decentralized applications. Our solution fulfills all the requirements put forth by Section 12A ff. of Schedule 2 to the AMLO while additionally guaranteeing the highest degree of customer privacy through the use of zero-knowledge proofs and verification interoperability throughout the market with the use of on-chain tokenization of customer credentials. For more details on the solution, please visit our website under www.zk.me.

We value regulatory compliance and work diligently to help companies in this industry maintain the highest standards of governance. We strongly believe that regulatory clarity, with simple, straightforward guidelines will be a major catalyst for further innovation and growth. Hong Kong has the potential to become the world's leading hub for VA and the decentralized finance markets of tomorrow. We believe that the disruptive growth potential of VATPs offering their customers access to not only virtual assets but also decentralized financial instruments (Lending, Derivatives, Asset Management) built on top of VA, cannot be overstated and we welcome the SFC take first steps in recognizing and embracing this growing industry.

We understand the importance of your role as a regulator in ensuring a fair and transparent market for all stakeholders. We welcome the opportunity to provide our feedback and insights on the consultation paper, and we hope that our response will contribute to the development of effective policies and regulations for the industry. We have carefully reviewed the consultation paper and have identified two areas where we believe we can provide valuable input. Our response will be based on our experience as a market participant, and we will strive to provide constructive and practical recommendations that will help achieve the objectives of the proposed regulations.

On the following pages, we provide detailed comments and views to the questions put forward regarding the provision of VA-based services to retail investors (Question 1), and most importantly, and pertaining to our expertise, we provide our view on how the recognition and use of modern technologies such DID and ZKP can ensure that the requirements laid out in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASP be implemented with the highest degree of efficiency, security and risk minimization (Question 9). We postulate that governance of decentralized financial instruments running on public distributed ledgers (DeFi) is not possible without the use of technical solutions that are decentralized and privacy preserving themselves. We invite you and the industry as a whole, to assess the disruptive capabilities of web3 native RegTech solutions over the coming years.

Thank you for considering our response, and we look forward to continuing our dialogue with your organization.

Best regards,

Question 1:
Do you agree that licensed platform operators should be allowed to provide their services to retail investors, subject to the robust investor protection measures proposed? Please explain your views.

zkMe response to Question 1:

zkMe welcomes retail investor participation under the new VATP guidelines. There are several factors to consider:

Relative importance of the retail sector in VA markets: Cutting retail investors off from this market will limit their exposure and ability to benefit from potential gains and opportunities arising from the new regulations taking effect this year. Retail investors are over-proportionally important to the global VA market, holding over 20% of the global virtual asset market. Retail investors will, if protected through the application of appropriate governance mechanisms, contribute significantly to the growth of the Hong Kong VA market.

Growing importance of and demand for decentralized financial instruments for investment purposes: We believe that virtual assets, especially those provided by decentralized, smart contract based, financial services (DeFi), will be the strongest driving force for growth in the next bull cycle. We therefore strongly believe that it should be a priority for any regulatory framework to provide a clear framework that allows for the creation of efficient, VATP controlled, permissioned DeFi front ends with seamless retail and institutional investor onboarding.

Overall, while it is important to ensure that robust investor protection measures are in place and they might be harder to implement for virtual assets, we believe that licensed platform operators should be allowed to provide their services to retail investors in the VA market, as this could help to promote market growth and provide retail investors with greater investment opportunities. We believe that mature technical solutions exist to help implement retail investor protection measures in VA and VA derivative markets (see our response to Question 9 for further details).

Sensible regulation that protects the individual investor (from privacy concerns, from unreliable intermediaries, from bad actors) while providing them direct access to virtual assets and decentralized financial services, is direly needed. Hong Kong has the opportunity to be a first mover in defining the global reference for VA investments. In such a regulatory sunrise period, it could establish itself as the global hub for VA and DeFi.

Question 9:
Do you have any comments on the requirements for virtual asset transfers or any other requirements in Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs? Please explain your views.

zkMe response to Question 9:

Our company welcomes the "same business, same risks, same rules" principle being applied to VATP. We support the implementation of AML/CFT recommendations by the FATF, especially the early implementation of the Crypto Travel Rule. As a global first to set comprehensive standards, we believe Hong Kong is quickly becoming an attractive hub of operations for forward-thinking VATPs.

To enable efficient handling of AML provisions in highly automated and decentralized VA markets, especially for the ones controlled by smart contracts (DeFi), we would welcome the VATP guidelines to recognize the use of novel, blockchain-native verification technologies as mechanisms to ensure that the statutory AML/CFT requirements are implemented as efficiently as possible.

Our main concern lies with the application of legacy, off-chain AML/CFT screening solutions (so called eKYC solutions) as they are employed in more mainstream financial services today. We believe that the use of such solutions would impose undue inefficiencies, prohibitively high entry barriers, and competitive disadvantages for VATPs when trading VA-based financial instruments. This is especially true for VATPs that aim to offer decentralized, permissioned financial product (DeFi) offerings to their customer base.

Specifically, the following **issues with the application of existing eKYC** solutions for VA-based financial instruments (especially DeFi) will arise if not addressed appropriately:

1. **Lack of KYC/AML interoperability**
2. **Impossibility to implement governance for unhosted wallets**
3. **Prohibitive solution inefficiencies**
4. **Resulting VA market liquidity fragmentation**

Without the use of on-chain counterparty identification mechanisms, it is our strong belief that an implementation of the requirements set forth in Chapter 12, especially those referring to wallet to wallet Travel Rule requirements and the verification of wallet ownership of self-hosted or unhosted wallets in Paragraphs 12.14.1 to 12.14.3 are effectively impossible.

Without a shared, public, identity registry, licensed VATPs would have to maintain at least three separate ledgers to keep track of the transactions for i) the Originator request, ii) the Originator required KYB/KYC information and iii) the on-chain transaction itself in order to verify identities of any on-chain transaction. This requirement of having to build up secondary infrastructures on top of the original VA settlement layer is extremely costly, inefficient and error prone. Technically, there are issues of state conflicts arising between the centralized and decentralized ledger and also among the different (VATP specific) centralized ledgers, issues of interoperability and increased transaction costs. By building up centralized infrastructure redundancies for KYC and AML checks, the biggest value propositions of the settlement layer of virtual assets (time to

transaction finality, process efficiency, decentralization, full asset liquidity, and transparency) are negated. Each VATP would have to create their own VA "walled garden" to ensure compliance, fragmenting the global VA market and introducing unnecessary trade barriers.

Additionally, since anonymous transfer of ownership or control of a self-hosted wallet is extremely easy and can happen at any time and without notification; one-off verifications of "wallet ownership" are to be seen as ineffective. Thus exposing any VATP that uses traditional ownership verification methods and interacts with self-hosted wallets to potential money laundering schemes such as the ones described in Chapters 12.1.4 ff. of the Guideline on AML and CFT for LC and SFC-licensed VATPs. Such VATP would therefore have to ban any transaction from and to self-hosted wallets, thus extremely limiting the maximum VA liquidity they could attract (given that more than 50% of the global VA assets by value are stored in self-hosted wallets).

In order to make full use of the benefits of the blockchain settlement infrastructure VAs are based on (i.e the time to transaction finality, process efficiency, decentralization, full asset liquidity, and full transaction transparency), any business logic that processes VA (e.g. VA derivative trading, collateralization, and KYC/AML checks) also need to be built on top of the same settlement layer (i.e. needs to be on-chain rather than processed in competing off-chain infrastructures). Any VA market that does not allow for the business logic layer to be processed on-chain, will inevitably be less efficient than a market that does. The efficiency gain of fully on-chain VA markets is analogous to the effects of the introduction of High Frequency Trading (HTF) in the early 2000's. Just like HTF, on-chain, decentralized financial and governance instruments substantially improve market liquidity, narrow bid-offer spread, lower volatility, and make trading and investing cheaper for all market participants.

We therefore suggest that the following three technological advancements be recognized as potential **solution approaches** to fulfill the AML requirements set forth by Chapter 12 of the AML Guideline for LCs and SFC-licensed VASPs:

1. **Use of on-chain, decentralized Identity Identifiers (DID):**
   By minting permanent, non-transferrable, non-fungible tokens on-chain (so called soulbound identifiers or SBT DID), it is technically possible to bind an identity to a VA wallet address. This on-chain identity could function as public representation that acquisition of required information for AML/CFT screening purposes (KYC/KYB processes) has taken place. A wallet address with a "KYC-pass" identity can therefore universally be considered whitelisted for participation in licensed VATP service offerings. SBT DID build trust and allow for global interoperability of AML/CFT screenings among all VA market participants.

   There is also a natural synergy between electronic Identity (eID) schemes and wallet-bound identities. A verified credential Issuer entrusted by the Immigration Department (or equivalently trusted government entity), could issue standardized, confirmations that the onboarding requirements laid out by Paragraphs 9.3 to 9.7 of the the VATP Guidelines including i) KYC information gathering, ii) standardized knowledge assessments, iii) risk tolerance and risk profile evaluations and iv) exposure limits determinations have been fulfilled directly to the user's on-chain wallet address. This would directly eliminate any risk of identity fraud introduced through false-positive verification results introduced by 3rd-party eKYC service providers. These on-chain representations would be visible to all participants and would ensure that a retail investor with an identified low risk tolerance and no service-specific knowledge nor training not be whitelisted for participation in that kind of service directly by any service provider without that specific service provider having to reprocess their own risk evaluation.

2. **Use of zero-knowledge proofs (ZKP= for identity verifications:**
   Zero-knowledge proofs (ZKP) are cryptographically verifiable proofs that a certain factual statement is true without disclosing the underlying facts. For example, with ZKP you could (for example) prove that a retail investor has passed AML/KYC background checks to all market participants without disclosing any of the underlying retail investor personal identifiable information (PII) such as Name and residence address. ZKPs act as privacy-preserving mechanisms for the day to day operations, only exposing relevant anonymized eligibility criteria, while still allowing for full plaintext identity disclosure where and if required by the regulator.

   Such "universally verifiable" levels of KYC proofs are unobtainable in current mainstream finance markets and a key reason why we believe regulators will have to embrace decentralized financial service offerings to protect retail investor integrity in the long term. With digital identity verifications, every single VA transaction between licensed VATP would be traceable, verifiably protected and secure. With the additional use of zero-knowledge technologies, these on-chain representations would be anonymized in order to ensure the privacy of all the stakeholders without losing any of the proofs' validity.

   Through the use of DID and ZKP verifications of user credentials, it is possible to implement robust investor protection measures for VA transactions on par if not exceeding those employed in mainstream finance. Other regulatory bodies are starting to officially recognize the benefits of DID and ZKP. The EU parliament for example has, in a world's first, recently passed and approved the use of ZKP for all identity verifications incl. KYC checks as part of their new European Digital Identification (eID) framework and their plans to develop what will be known as the European Digital Identity Wallet. We highly recommend the Hong Kong regulatory bodies to consider such decentralized and anonymous customer credential verifications for VATP KYC/AML checks.

3. **Use of on-chain Travel Rule implementation:**
   Using on-chain Identities makes the implementation of travel rule requirements for VA transactions very easy. Rather than setting up parallel channels for the processing of on-chain transactions and off-chain obtaining of required counterparty information, the VATP handling the Originator side, would just send a copy of the on-chain identity together with the VA on-chain transaction to the Recipient wallet. Since the on–chain identities are visible to all participants, it would make it very easy to identify which wallets (be them hosted or unhosted) fulfill AML/CTF requirements even before any transaction is initiated. An extremely lean solution for an extremely technically challenging solution if solved off-chain.

At zkMe, we believe that the gradual introduction of decentralized technologies for the governance of VA trading providers will ensure that Hong Kong establishes itself as the world's leading hub for VA and VA derivative trading.